COMPUTATION OF ATR DARMON POINTS ON NON-GEOMETRICALLY MODULAR ELLIPTIC CURVES

XAVIER GUITART AND MARC MASDEU

Abstract. ATR points were introduced by Darmon as a conjectural construction of algebraic points on certain elliptic curves for which in general the Heegner point method is not available. So far the only numerical evidence, provided by Darmon–Logan and Gärtner, concerned curves arising as quotients of Shimura curves. In those special cases the ATR points can be obtained from the already existing Heegner points, thanks to results of Zhang and Darmon–Rotger–Zhao.

In this paper we compute for the first time an algebraic ATR point on a curve which is not uniformizable by any Shimura curve, thus providing the first piece of numerical evidence that Darmon's construction works beyond geometric modularity. To this purpose we improve the method proposed by Darmon and Logan by removing the requirement that the real quadratic base field be norm-euclidean, and accelerating the numerical integration of Hilbert modular forms.

1. Introduction

Let F be a totally real number field and let E/F be an elliptic curve of conductor $\mathfrak{N}$. Denote by $L(E/F,s)$ the Hasse–Weil L-series attached to E, which is known to converge in the half plane $\Re(s) > 3/2$. Let us assume thorough this note that E is *modular*; that is to say, that $L(E/F,s)$ equals the L-series of a Hilbert modular form over F of weight 2 and level $\mathfrak{N}$. Thanks to the modularity theorems of [Wil95], [BCDT01] and [SW01], E is known to be modular if either $F=\mathbb{Q}$, or if $[F\colon \mathbb{Q}]>1$ and it satisfies certain mild conditions on the reduction type at primes above 3. The L-series $L(E/F,s)$ admits analytic continuation, and the Birch and Swinnerton-Dyer (BSD) Conjecture predicts that its order of vanishing at $s=1$, called the *analytic rank* of E/F, equals the rank of the group of F-rational points $E(F)$.

In this context, BSD Conjecture is known to hold in analytic rank 0 or 1 provided that E satisfies the following *Jacquet–Langlands hypothesis*:

(JL) Either $[F\colon \mathbb{Q}]$ is odd or there is a prime $\mathfrak{p}$ in F such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{N})$ is odd.

Theorem 1.1 (Gross–Zagier, Kolyvagin, Zhang)**.** *Let E be a modular elliptic curve over a totally real number field F satisfying (JL). If $\mathrm{ord}_{s=1} L(E/F,s) \leq 1$ then*

$$\mathrm{ord}_{s=1} L(E/F,s) = \mathrm{rank}(E(F)).$$

In analytic rank 0, BSD is also known for modular elliptic curves not satisfying (JL), thanks to the work of Longo [Lon06]. However, in analytic rank 1 (JL) cannot be dispensed with at the moment, because the construction of non-torsion points

Date: October 9, 2012.

2010 *Mathematics Subject Classification.* 11G40 (11F41, 11Y99).

relies on the existence of the so-called Heegner points. Indeed, if E satisfies (JL) then it is *geometrically modular*: there exists a non-constant F-homomorphism

$$\pi_E\colon \operatorname{Jac}(X) \longrightarrow E, \tag{1.1}$$

from the Jacobian of a suitable Shimura curve X defined over F onto E. Shimura curves are endowed with CM points, which are defined over ring class fields of quadratic CM extensions K/F. The projection of CM points via π_E gives rise to Heegner points on E, whose arithmetic behavior is linked to the corresponding L-series of E thanks to formulas of Gross–Zagier and Zhang.

On the other hand, if E does not satisfy (JL) then it is not known to be geometrically modular unless it is a $\mathbb{Q}$-*curve*; i.e., a curve isogenous to all of its Galois conjugates. As a consequence of Serre's modularity conjecture $\mathbb{Q}$-curves admit $\overline{\mathbb{Q}}$-parametrizations from classical modular Jacobians, and this has been exploited in [DRZ12] in order to construct Heegner points and prove BSD in analytic rank 1 for some $\mathbb{Q}$-curves not satisfying (JL). But BSD in analytic rank 1 seems to remain intractable for elliptic curves which are not $\mathbb{Q}$-curves and do not satisfy (JL). Indeed, since they are not geometrically modular the Heegner point method sketched in the previous paragraph cannot be applied in this setting.

The Heegner point construction constitutes the only known procedure for systematically manufacturing algebraic non-torsion points on elliptic curves. However, several *conjectural* constructions have emerged in the last years under the generic name of *Stark–Heegner points*, or also *Darmon points* as the first such construction was introduced in [Dar01]. Variants of this initial construction applying to several different settings have been proposed since then, for instance in [Das05], [Gre09], [LRV09], [Gär11a], and [GRZ12]. The leitmotif of these methods is the analytic construction of algebraic points on ring class fields of quadratic extensions K/F which, unlike the classical case, are not CM.

This note deals with the effective computation of a type of Darmon points known as *ATR points*, which where introduced in [Dar04, Chapter VIII]. To explain the terminology, recall that a number field is said to be *almost totally real*, or *ATR* for short, if it has exactly one complex non-real archimedean place.

Let K be a quadratic ATR extension of the totally real field F. For an ideal $\mathfrak{c}$ of F denote by $R_{\mathfrak{c}} \subset K$ the order of conductor $\mathfrak{c}$, and $H_{\mathfrak{c}}$ the ring class field corresponding to $R_{\mathfrak{c}}$. Darmon associates to any optimal embedding $\varphi\colon R_{\mathfrak{c}} \hookrightarrow \mathrm{M}_2(\mathcal{O}_F)$ a point $P_\varphi \in E(\mathbb{C})$, called an *ATR point*, which is conjectured to be defined over $H_{\mathfrak{c}}$. Moreover, by analogy with the formulas of Gross–Zagier and Zhang, its trace down to K is believed to be non-torsion if and only if $\operatorname{ord}_{s=1} L(E/K,s) = 1$.

An algorithm for computing ATR points in the particular case where F is real quadratic and E has conductor 1 is given in [DL03]. These elliptic curves do not satisfy (JL), so that the Heegner point construction is not available in general. Both the definition of the points P_φ and the conjectures of Darmon concerning them will be recalled in Section 2. For the moment, it is enough for us to mention that they are the image under the Weierstrass map $\mathbb{C}/\Lambda_E \to E(\mathbb{C})$ of a complex number of the form

$$J_\varphi = \int_{a_1}^{b_1}\int_{c_1}^{d_1} \omega + \cdots + \int_{a_n}^{b_n}\int_{c_n}^{d_n} \omega, \tag{1.2}$$

where ω is a certain differential 2-form on the Hilbert modular surface $\mathrm{SL}_2(\mathcal{O}_F)\backslash\mathcal{H}^2$. The limits of integration depend on the embedding φ, but they are not uniquely

determined: for a given φ there are many possible choices for a_i, b_i, c_i, d_i. The Fourier series of ω is explicitly computable from E, and term by term integration of a truncation leads to a numerical approximation to J_φ. The rate of convergence depends essentially on the imaginary parts of the limits, and this turns out to be the main computational restriction of this method.

The algorithm outlined above was used in [DL03] to obtain numerical evidence towards Darmon's conjectures. More concretely, ATR points on three concrete elliptic curves were computed, and they were checked to be (up to a certain numerical precision) multiples of the corresponding generators of the Mordell–Weil groups. Calculations of the same kind were performed in [Gär11b] for one more curve. However, computational limitations restricted them to elliptic curves which all happen to be geometrically modular. In this case, the BSD Conjecture implies that ATR points in these curves should be related to the already existing Heegner points. Actually, in the case of $\mathbb{Q}$-curves (as they are all examples considered in [DL03]) a precise relation between Heegner and ATR points is conjectured in [DRZ12, §4.2].

In this note we speed up the algorithm devised by Darmon and Logan by improving its two main bottlenecks. Namely, the computation of integrals of Hilbert modular forms, and the determination of limits a_i, b_i, c_i, d_i in (1.2) having the highest imaginary part possible. This allows us to gather more numerical evidence in support of Darmon's conjectures, by calculating ATR points on elliptic curves which were not computationally accessible using the algorithm in [DL03]. In particular, we have been able to compute for the first time an ATR point of infinite order on a *non-geometrically modular* elliptic curve.

More concretely, the contents of the article are as follows. In Section 2 we review the definition of the points P_φ and Darmon's conjectures on their arithmetic properties. We also sketch the algorithm of Darmon and Logan for their explicit computation.

In Section 3 we present the algorithm for speeding up the computation of integrals of Hilbert modular forms. The idea is to use the fact that the limits are invariant under the group $\mathrm{SL}_2(\mathcal{O}_F)$ in order to transform the given integral into a sum of integrals whose limits are uniformly bounded away from the real axis, the bound depending only on F. It is worth remarking that this algorithm does not exploit any particular property of the integrals involved in ATR points, and therefore it may be of independent interest for computing integrals of Hilbert modular forms in other contexts.

In Section 4 we comment on a trick that can sometimes accelerate the computation of ATR points. The procedure for computing the limits a_i, b_i, c_i, d_i in (1.2) for an embedding φ involves at some point the calculation of a continued fraction expansion of an element in F. We exploit the non-uniqueness of continued fractions to attach to a given φ limits a_i, b_i, c_i, d_i with as high imaginary part as possible.

Finally, in Section 5 we use Darmon–Logan's algorithm together with the improvements of sections 3 and 4 to enlarge the pool of elliptic curves on which Darmon's conjectures have been numerically tested. Arguably, the most interesting among them is the curve E_{509} given by the equation

$$y^2 - xy - \omega y = x^3 + (2+2w)x^2 + (162+3w)x + (71+34\omega), \quad \omega = \frac{1+\sqrt{509}}{2},$$

because it is not a $\mathbb{Q}$-curve. We have computed an ATR point corresponding to the field $K = F(\sqrt{9144\omega + 98577})$, and we have numerically checked that it coincides with a multiple of the Mordell–Weil generator of $E_{509}(K)$. Since E_{509} is not geometrically modular, such point does not seem to be explained by the presence of Heegner points. This gives experimental evidence that Darmon's construction leads to algebraic points that are genuinely new, not attainable by classical methods.

Finally, it is worth mentioning that ATR points are also the base of an algorithm by L. Dembélé [Dem08] for computing equations of elliptic curves with everywhere good reduction attached to Hilbert modular forms of level 1. The authors hope that the algorithm presented in this note can be useful for this purpose, and that it may lead in the future to a systematic computation of such equations using Dembélé's method.

Acknowledgments. The authors are thankful to Henri Darmon and Victor Rotger for initially suggesting the problem and for many helpful conversations, and to the anonymous referee for many valuable comments and suggestions. They are grateful to the Max Planck Institute for Mathematics for the hospitality and financial support, and for making available its computational resources, crucially needed for part of this note. Part of this work was also carried out in the facilities of Centro de Ciencias de Benasque Pedro Pascual during the Summer of 2011. The authors received financial support from DGICYT Grant MTM2009-13060-C02-01 and from 2009 SGR 1220.

2. Computation of ATR points

Let F be a real quadratic number field of discriminant D and narrow class number 1. Write $\mathcal{O}_F$ for its ring of integers and set $\Gamma = \mathrm{SL}_2(\mathcal{O}_F)$. We denote by v_0, v_1 the embeddings of F into $\mathbb{R}$. For an element $x \in F$ we may write x_i instead of $v_i(x)$, and $|x|$ for the norm of x, given by x_0x_1. Recall that Γ acts discretely on $\mathcal{H}^2$ via $v_0 \times v_1$. The analytic variety $\Gamma \setminus \mathcal{H}^2$ can be compactified by adding one cusp, which gives rise to the Hilbert modular surface X attached to Γ.

Let K/F be a quadratic ATR extension. For an ideal $\mathfrak{c}$ of F we denote by $H_{\mathfrak{c}}$ the ring class field corresponding to the order $R_{\mathfrak{c}}$ of conductor $\mathfrak{c}$ of K. We assume without loss of generality that v_0 extends to a complex place of K and v_1 extends to a pair of real places of K. We fix an extension of v_0 to $\overline{\mathbb{Q}} \subset \mathbb{C}$, which we use to to identify K and its extensions with subfields of $\mathbb{C}$. Recall that an embedding of $\mathcal{O}_F$-algebras $\varphi\colon R_{\mathfrak{c}} \hookrightarrow M_2(F)$ is said to be *optimal* if $\varphi(K) \cap M_2(\mathcal{O}_F) = \varphi(R_{\mathfrak{c}})$. We denote by $\mathcal{E}_{\mathfrak{c}}$ the set of such optimal embeddings.

Let E/F be an elliptic curve of conductor 1. In this section we review Darmon's construction, which attaches to each optimal embedding φ a point $P_\varphi \in E(\mathbb{C})$ that conjecturally belongs to $E(H_{\mathfrak{c}})$. There are several equivalent ways of defining P_φ. For instance, a nice geometric definition in terms of a non-algebraic analogue to the Abel–Jacobi map is given in [DRZ12, §2.1]. However, for computational purposes the original definition of [Dar04, Chapter VIII], or rather the subsequent refinement of [DL03] are better suited. Key to the approach of [DL03] is the definition of certain *semi-definite integrals* of Hilbert modular forms, whose existence and main properties we will take as a black box.

2.1. Semi-definite integrals of Hilbert modular forms.

Let $f \in S_2(\Gamma)$ be a Hilbert modular form. Recall that f has a Fourier expansion indexed by totally

positive elements of $\mathcal{O}_F$. Actually, the Fourier coefficient corresponding to $n \in \mathcal{O}_F^+$ only depends on the ideal (n) generated by n, and the expansion is of the form

$$f(\tau_0, \tau_1) = \sum_{n \in \mathcal{O}_F^+} a_{(n)} e^{2\pi i (\frac{n_0}{\delta_0}\tau_0 + \frac{n_1}{\delta_1}\tau_1)}, \quad \tau_0, \tau_1 \in \mathcal{H}, \tag{2.1}$$

where $\delta_i = v_i(\delta_F)$ and δ_F is a totally positive generator of the different ideal of F. Let us assume from now on that all Fourier coefficients $a_{(n)}$ are rational numbers. The reader can refer to [GRZ12, §2.4] for the definition of ATR points when the Fourier coefficients generate a number field of degree > 1, in which case they belong to some higher dimensional modular abelian variety.

The differential form

$$\omega_f = \frac{(2\pi i)^2}{\sqrt{D}} f(\tau_0, \tau_1) d\tau_0 d\tau_1$$

is invariant under the action of Γ and extends to a holomorphic form at the cusp, thus defining a holomorphic 2-form on X. The expansion in Equation (2.1) is useful for computing integrals of ω_f. Indeed, for $x_0, x_1, y_0, y_1 \in \mathcal{H}$ we have that

$$\int_{x_0}^{y_0} \int_{x_1}^{y_1} \omega_f = \sqrt{D} \sum_{n \in \mathcal{O}_F^+} \frac{a_{(n)}}{|n|} \left(e^{2\pi i \frac{n_0}{\delta_0} y_0} - e^{2\pi i \frac{n_0}{\delta_0} x_0} \right) \left(e^{2\pi i \frac{n_1}{\delta_1} y_1} - e^{2\pi i \frac{n_1}{\delta_1} x_1} \right). \tag{2.2}$$

In the definition of ATR points the key role is not played by ω_f but instead by the non-holomorphic differential

$$\omega_f^+ = \frac{(2\pi i)^2}{\sqrt{D}} \Big(f(\tau_0, \tau_1) d\tau_0 d\tau_1 + f(u_0\tau_0, u_1\overline{\tau}_1) d(u_0\tau_0) d(u_1\overline{\tau}_1) \Big),$$

where u is a fundamental unit in F such that $u_0 > 1$ and $u_1 < -1$. The differential form ω_f^+ is also Γ-invariant, and it follows from the definition that it is invariant under the action of the matrix $\tilde{\gamma}_u = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$. Therefore, if we let

$$\tilde{\Gamma} = \{\gamma \in \mathrm{GL}_2(\mathcal{O}_F) \ : \ v_0(\det(\gamma)) > 0\}$$

we find that

$$\int_{x_0}^{y_0} \int_{x_1}^{y_1} \omega_f^+ = \int_{\gamma x_0}^{\gamma y_0} \int_{\gamma x_1}^{\gamma y_1} \omega_f^+, \quad \text{for all } \gamma \in \tilde{\Gamma}.$$

Here γ acts on the outer limits (reps. inner limits) through v_0 (resp. v_1).

Let

$$\Lambda_f^+ = \left\{ \int_\delta \omega_f^+ \ : \delta \in H_2(X, \mathbb{Z}) \right\} \subset \mathbb{C}$$

be the period lattice of ω_f^+.

Theorem 2.1 (Darmon–Logan)**.** *There exists a unique map*

$$\begin{array}{ccc} \mathcal{H} \times \mathbb{P}^1(F) \times \mathbb{P}^1(F) & \longrightarrow & \mathbb{C}/\Lambda_f^+ \\ (\tau_0, c_1, c_2) & \longmapsto & \int^{\tau_0} \int_{c_1}^{c_2} \omega_f^+ \end{array}$$

satisfying the following properties:

(i) $\int^{\gamma\tau_0} \int_{\gamma c_1}^{\gamma c_2} \omega_f^+ = \int^{\tau_0} \int_{c_1}^{c_2} \omega_f^+$ *for all* $\gamma \in \tilde{\Gamma}$,

(ii) $\int^{\tau_0} \int_{c_1}^{c_2} \omega_f^+ + \int^{\tau_0} \int_{c_2}^{c_3} \omega_f^+ = \int^{\tau_0} \int_{c_1}^{c_3} \omega_f^+$,

(iii) $\int^{y} \int_{c_1}^{c_2} \omega_f^+ - \int^{x} \int_{c_1}^{c_2} \omega_f^+ = \int_x^y \int_{c_1}^{c_2} \omega_f^+$.

For the existence of such map we refer the reader to [DL03, §1]. Uniqueness is proved in [DL03, §4], and it follows from repeated application of properties (i), (ii) and (iii). Since this also leads to an algorithm for computing the map, we review the proof in the next section.

2.2. **Computation of semi-definite integrals via continued fractions.** Given $b_0, b_1, \ldots, b_n \in \mathcal{O}_F$ the (finite) *continued fraction* $[b_0, b_1, \ldots, b_n] \in F$ is defined, inductively, as

$$[b_0] = b_0,\ [b_0, b_1] = b_0 + \frac{1}{b_1}, \ldots, [b_0, b_1, \ldots, b_n] = [b_0, [b_1, \ldots, b_n]].$$

Let $[b_0, b_1, \ldots, b_k] = \frac{p_k}{q_k}$, with $p_k, q_k \in \mathcal{O}_F$ coprime. It is well known that

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}. \tag{2.3}$$

Since $\mathcal{O}_F^\times$ is infinite and F has trivial class number, by a result of Cooke–Vaserstein [Coo76] every element $c \in F$ can be written as a finite continued fraction. See [GM12] and §4 for an effective version of this result.

Two cusps $c_1, c_2 \in \mathbb{P}^1(F)$ are said to be *adjacent* if $c_1 = \gamma \cdot 0$ and $c_2 = \gamma \cdot \infty$ for some $\gamma \in \Gamma$. One can join every cusp $c \in F$ with ∞ by a sequence of adjacent cusps. Indeed, if $c = [b_0, b_1, \ldots, b_n]$ then the sequence

$$\infty, \frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} = c$$

has this property thanks to (2.3). Using this fact and property (i) every integral $\int^{\tau_0} \int_{c_1}^{c_2} \omega_f^+$ can be written as a sum of integrals of the form $\int^{\tau_0} \int_{\gamma\cdot 0}^{\gamma\cdot\infty} \omega_f^+$. Thanks to (i) they are of the form $\int^{\tau} \int_0^\infty \omega_f^+$, and can be computed as follows:

$$\begin{aligned}\int^{\tau} \int_0^\infty \omega_f^+ &= \int^{\tau} \int_0^1 \omega_f^+ + \int^{\tau} \int_1^\infty \omega_f^+ \\ &= \int^{-\frac{1}{\tau}} \int_\infty^{-1} \omega_f^+ + \int^{\tau-1} \int_0^\infty \omega_f^+ \\ &= \int_{1-\frac{1}{\tau}}^{\tau-1} \int_0^\infty \omega_f^+.\end{aligned}$$

Integrals of the form $\int_{\tau_1}^{\tau_2} \int_0^\infty \omega_f^+$, with $\tau_1, \tau_2 \in \mathcal{H}$, can be computed by taking $\tau_3 \in \mathcal{H}$ and writing

$$\int_{\tau_1}^{\tau_2} \int_0^\infty \omega_f^+ = \int_{\tau_1}^{\tau_2} \int_0^{\tau_3} \omega_f^+ + \int_{\tau_1}^{\tau_2} \int_{\tau_3}^\infty \omega_f^+ = \int_{-\frac{1}{\tau_1}}^{-\frac{1}{\tau_2}} \int_\infty^{-\frac{1}{\tau_3}} \omega_f^+ + \int_{\tau_1}^{\tau_2} \int_{\tau_3}^\infty \omega_f^+, \tag{2.4}$$

for which formula (2.2) can be used.

2.3. **Definition of ATR points.** Under the assumption that E is modular there exists a Hilbert modular newform $f_E \in S_2(\Gamma)$ such that $L(E/F, s) = L(f_E, s)$. The Fourier expansion of f_E can be explicitly computed as follows. For a prime ideal $\mathfrak{p} \subset F$, let $a_\mathfrak{p} := |\mathfrak{p}| + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$, where $|\mathfrak{p}|$ denotes $\#\mathcal{O}_F/\mathfrak{p}$. For arbitrary ideals $\mathfrak{n} \subset F$ the integer $a_\mathfrak{n}$ is defined by means of the identity

$$\sum_{\mathfrak{n} \subset F} a_\mathfrak{n} |\mathfrak{n}|^{-s} = \prod_{\mathfrak{p} \text{ prime}} \left(1 - a_\mathfrak{p} |\mathfrak{p}|^{-s} + |\mathfrak{p}|^{1-2s}\right)^{-1},$$

and the Fourier expansion of f_E is given by

$$f_E(\tau_0,\tau_1) = \sum_{n\in\mathcal{O}_F^+} a_{(n)} e^{2\pi i(\frac{n_0}{\delta_0}\tau_0 + \frac{n_1}{\delta_1}\tau_1)}, \quad \tau_0,\tau_1 \in \mathcal{H}. \tag{2.5}$$

Let $\varphi\colon R_{\mathfrak{c}} \hookrightarrow M_2(F)$ be an optimal embedding. Since K is ATR the group

$$\Gamma_\varphi = \{\gamma \in \varphi(\mathcal{O}_F) \ : \ \det(\gamma) = 1\}$$

has rank 1; let γ_φ be one of its generators. Since v_0 extends to a complex place of K, the action of $K^\times$ on $\mathcal{H}$ by means of $v_0 \circ \varphi$ has a single fixed point τ_0. Let J_φ be the quantity in $\mathbb{C}/\Lambda_f^+$ defined as

$$J_\varphi = \int^{\tau_0} \int_\infty^{\gamma_\varphi \infty} \omega_f^+. \tag{2.6}$$

Let $\omega_E \in H^0(E,\Omega^1)$ be a differential which extends to a smooth differential on the Néron model of E over $\mathcal{O}_F$. Let

$$\Lambda_i = \left\{ \int_Z v_i(\omega_E) \ : \ Z \in H_1(E_j,\mathbb{Z}) \right\}$$

and let λ_j^+ (resp. λ_j^-) be a generator of $\Lambda_j \cap \mathbb{R}$ (resp. $\Lambda_j \cap i\mathbb{R}$).

Conjecture 2.2 (Oda)**.** *There exists a integer c such that $\frac{c}{\lambda_1^+}\Lambda_f^+ \subseteq \Lambda_0$.*

Granting Conjecture 2.2 and denoting by $\eta\colon \mathbb{C}/\Lambda_0 \to E_0(\mathbb{C})$ the Weierstrass parametrization map, the ATR point P_φ is defined as

$$P_\varphi = \eta(\frac{c}{\lambda_1^+} \cdot J_\varphi) \in E_0(\mathbb{C}).$$

The group $\tilde{\Gamma}$ acts by conjugation on $\mathcal{E}_{\mathfrak{c}}$, and the set of equivalence classes $\mathcal{E}_{\mathfrak{c}}/\tilde{\Gamma}$ has cardinal $[H_{\mathfrak{c}}\colon K]$ (cf. [Dar04, §8.5]).

Conjecture 2.3 (Darmon)**.** *The point P_φ belongs to $E_0(H_{\mathfrak{c}})$. Moreover, the point*

$$P_K = \sum_{\varphi\in\mathcal{E}_{\mathfrak{c}}/\tilde{\Gamma}} P_\varphi$$

belongs to $E_0(K)$ and it is non-torsion if and only if $\operatorname{ord}_{s=1} L(E/K,s) = 1$.

Note that under the assumptions of this section, namely the conductor of E/F is 1 and K/F is ATR, the L-function $L(E/K,s)$ has sign -1. Thus the condition $\operatorname{ord}_{s=1} L(E/K,s) = 1$ is equivalent to $L'(E/K,1) \neq 0$, which can be numerically checked.

3. Integration of Hilbert Modular forms

When evaluating (2.2) one can collect the elements $n \in \mathcal{O}_F^+$ modulo powers of u^2, because the Fourier coefficient corresponding to n only depends on the ideal (n). The sum corresponding to $n \cdot \langle u^2 \rangle$ is then

$$S_n = \sqrt{D} \sum_{k=-\infty}^{\infty} \frac{a_{(n)}}{|n|} \left(e^{2\pi i \frac{n_0}{\delta_0} u_0^{2k} y_0} - e^{2\pi i \frac{n_0}{\delta_0} u_0^{2k} x_0} \right) \left(e^{2\pi i \frac{n_1}{\delta_1} u_0^{-2k} y_1} - e^{2\pi i \frac{n_1}{\delta_1} u_0^{-2k} x_1} \right).$$

For a fixed k, the modulus of each exponential term (after multiplying out the brackets) is of the form

$$e^{-2\pi(\frac{n_0}{\delta_0} r u_0^{2k} + \frac{n_1}{\delta_1} s u_0^{-2k})}, \quad \text{with } r \in \{\Im(y_0), \Im(x_0)\}, s \in \{\Im(y_1), \Im(x_1)\}. \tag{3.1}$$

It is easy to see that (3.1) has a single maximum, when viewed as a function of k, and that the maximum value afforded by the four exponential terms is bounded by

$$M_n = e^{\frac{-4\pi\sqrt{|n|}\epsilon}{\sqrt{D}}},$$

where $\epsilon = \epsilon(x_0, y_0, x_1, y_1)$ is defined by:

$$\epsilon(x_0, y_0, x_1, y_1)^2 = \min\{\Im(x_0)\Im(x_1), \Im(x_0)\Im(y_1), \Im(y_0)\Im(y_1), \Im(y_0)\Im(x_1)\}. \tag{3.2}$$

Moreover, one easily checks that S_n is dominated by a geometric series and that

$$S_n \leq \frac{2\sqrt{D}|a_{(n)}|M_n}{|n|}, \quad \text{for } |n| >> 0.$$

This estimate allows us to know a priori how many terms need to be considered in order to obtain a prescribed accuracy. We observe that the speed of convergence of expression (2.2) depends on the limits x_0, y_0, x_1, y_1 through the quantity $\epsilon(x_0, y_0, x_1, y_1)$. The main result of this section is the following.

Theorem 3.1. *There exists a constant ϵ_F, which depends only on F, such that for every $(x_0, y_0, x_1, y_1) \in \mathcal{H}^4$ and for every $\epsilon_0 < \epsilon_F$ the integral $\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f$ can be expressed as*

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f = \int_{a_1}^{b_1}\int_{c_1}^{d_1} \omega_f + \cdots + \int_{a_n}^{b_n}\int_{c_n}^{d_n} \omega_f, \tag{3.3}$$

with $\epsilon(a_i, b_i, c_i, d_i) \geq \epsilon_0$ for all $i = 1, \ldots, n$.

Observe that in the integrals considered in Theorem 3.1 the four limits of integration lie in $\mathcal{H}$. By (2.4) integrals of the form $\int_{x_0}^{y_0}\int_{x_1}^{\infty} \omega_f^+$ are involved in the computation of ATR points. One can choose any $y_1 \in \mathcal{H}$ whose imaginary part is large enough to satisfy that

$$\int_{x_0}^{y_0}\int_{x_1}^{\infty} \omega_f^+ = \int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f^+ + \int_{x_0}^{y_0}\int_{y_1}^{\infty} \omega_f^+, \quad \text{with } \Im(x_0)\Im(y_1), \Im(y_0)\Im(y_1) > \epsilon_F,$$

and apply Theorem 3.1 to the integral $\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f^+$.

We devote the rest of the section to prove Theorem 3.1, which as we will see can be made effective and algorithmic.

It will be useful for us to regard F as a subset of $\mathbb{R}^2$ by means of $v_0 \times v_1$. Let $\|\cdot\|$ denote the norm on $\mathbb{R}^2$ given by

$$\|(x_0, x_1)\| = \max\{|x_0|, |x_1|\}.$$

The basic ingredient in the proof of 3.1 is the following classical result.

Lemma 3.2. *There exists a constant C_F, only depending on F, such that for each $x \in \mathbb{R}^2$ and for each $0 < \delta < 1$ there are elements $c, d \in \mathcal{O}_K$, with $c \neq 0$, such that*

$$\|cx + d\| \leq \delta, \quad \|c\| \leq \frac{C_F}{\delta}.$$

Proof. This is [Fre90, Lemma 3.6]. We rewrite the proof in an algorithmic fashion in order to give an approximation to C_F (see Remark 3.3 below), as well as to give an algorithm to find the elements c and d.

Consider a fundamental parallelogram P for $\mathcal{O}_F$ as a subgroup of $\mathbb{R}^2$. Let $U_1, \ldots, U_N$ be boxes of side δ that cover P. It is easy to see that there is a constant N', depending only on F, such that N can be taken to be $\leq N'/\delta^2$.

For each positive real r, consider the set

$$S_F(r) = \{c \in \mathcal{O}_F \mid \|c\| < r\}.$$

A well-known result in Ehrhart theory (see e.g. [BR07, Theorem 2.9]) implies that there exists a constant $C_F > 0$, which depends on F but not on δ, such that

$$\#S_F\left(\frac{C_F}{2\delta}\right) > \frac{N'}{\delta^2} \geq N.$$

Consider now an ordering $\{c_n\}_{n\geq 1}$ of the elements of $S_F(C_F/(2\delta))$. For each of the c_n, find $d_n \in \mathcal{O}_F$ such that

$$c_n x + d_n \in P,$$

and set $i(n)$ to be the integer such that $c_n x + d_n \in U_{i(n)}$. By the pigeonhole principle the sequence $\{i(n)\}_n$ will have a repetition, say $i(n_1) = i(n_2)$. Therefore

$$\|(c_{n_1} - c_{n_2})x + (d_{n_1} - d_{n_2})\| < \delta,$$

and

$$\|c_{n_1} - c_{n_2}\| \leq \|c_{n_1}\| + \|c_{n_2}\| \leq \frac{C_F}{2\delta} + \frac{C_F}{2\delta} = \frac{C_F}{\delta}.$$

The seeked elements are thus $c = c_{n-1} - c_{n-2}$ and $d = d_{n-1} - d_{n-2}$. □

Remark 3.3. In our applications, the parameter δ will be small enough so that the quantity N in the above proof can be approximated by $\mathrm{area}(P)/\delta^2$. Also, [BR07, Theorem 2.9(b)] gives in this case that

$$\#S_F\left(\frac{r}{2\delta}\right) \geq \frac{r^2}{4\delta^2}\frac{4}{\mathrm{area}(P)} + 1.$$

Therefore, it is enough for $\#S_F(\frac{r}{2\delta})$ to be larger than N that

$$\frac{r^2}{4\delta^2}\frac{4}{\mathrm{area}(P)} \geq \frac{\mathrm{area}(P)}{\delta^2}.$$

This yields an approximate value of $C_F \approx \mathrm{area}(P)$, which is good enough for our purposes. Note that this area is easily calculated: if $\mathcal{O}_F = \mathbb{Z} \oplus \mathbb{Z}w$, then $\mathrm{area}(P) = |w_0 - w_1|$.

We define

$$\epsilon_F = \frac{u_0}{C_F(1 + u_0^2)}.$$

In the next lemmas we prove that this can, indeed, be taken as the constant ϵ_F of Theorem 3.1.

Lemma 3.4. *Let $z = (z_0, z_1)$ be an element in $\mathcal{H} \times \mathcal{H}$. There exists a matrix $\gamma \in \Gamma$ such that*

$$(\Im(\gamma_0 z_0)\Im(\gamma_1 z_1))^{1/2} \geq \epsilon_F.$$

Proof. Let $z_j = r_j + is_j$ and let $r = (r_0, r_1)$. If $s_0 s_1 \geq \epsilon_F^2$ one may take $\gamma = 1$ and there result is obvious, so assume from now on that $s_0 s_1 < \epsilon_F^2$. By Lemma 3.2 for each $0 < \delta < 1$ there exist $c', d' \in \mathcal{O}_F$ with $c' \neq 0$ and such that

$$\|c'r + d'\| \leq \delta, \quad \|c'\| \leq \frac{C_F}{\delta}.$$

We have that

$$\left((c_0' r_0 + d_0')^2 + c_0'^2 s_0^2\right)\left((c_1' r_1 + d_1')^2 + c_1'^2 s_1^2\right) \leq \left(\delta^2 + \frac{C_F^2 s_0^2}{\delta^2}\right)\left(\delta^2 + \frac{C_F^2 s_1^2}{\delta^2}\right).$$

Let $g = \gcd(c', d')$ and let $n = \mathrm{Nm}_{K/\mathbb{Q}}(g)$. If we let $c = c'/g$ and $d = d'/g$ then

$$\begin{aligned}\left((c_0 r_0 + d_0)^2 + c_0^2 s_0^2\right)\left((c_1 r_1 + d_1)^2 + c_1^2 s_1^2\right) &\leq \frac{1}{n^2}\left(\delta^2 + \frac{C_F^2 s_0^2}{\delta^2}\right)\left(\delta^2 + \frac{C_F^2 s_1^2}{\delta^2}\right) \\ &\leq \left(\delta^2 + \frac{C_F^2 s_0^2}{\delta^2}\right)\left(\delta^2 + \frac{C_F^2 s_1^2}{\delta^2}\right).\end{aligned}$$

Since $\gcd(c, d) = 1$ there exists $\gamma \in \Gamma$ having (c, d) as bottom row and

$$\begin{aligned}\Im(\gamma_0 z_0)\Im(\gamma_1 z_1) &= \frac{s_0}{|c_0 z_0 + d_0|^2}\frac{s_1}{|c_1 z_1 + d_1|^2} \\ &= \frac{s_0 s_1}{\left((c_0 r_0 + d_0)^2 + c_0^2 s_0^2\right)\left((c_1 r_1 + d_1)^2 + c_1^2 s_1^2\right)} \\ &\geq \frac{s_0 s_1}{\left(\delta^2 + \frac{C_F^2 s_0^2}{\delta^2}\right)\left(\delta^2 + \frac{C_F^2 s_1^2}{\delta^2}\right)}.\end{aligned}$$

We choose δ that maximizes this expression. The optimal value for δ turns out to be

$$\delta = (C_F^2 s_0 s_1)^{1/4}.$$

Note that $\delta < 1$ since $s_0 s_1 < \epsilon_F^2$. With this value of δ the above inequality gives

$$\left(\Im(\gamma_0 z_0)\Im(\gamma_1 z_1)\right)^{1/2} \geq \frac{1}{2C_F}\frac{G(s_0, s_1)}{A(s_0, s_1)},$$

where $G(s_0, s_1)$ and $A(s_0, s_1)$ are the geometric and arithmetic means, respectively. Of course, for this quantity to be not too small we should ensure that the ratio G/A is not too small. That is, s_0 and s_1 should be close. This can be done by the action of the matrix $\gamma_u = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$, which guarantees that:

$$u_0^{-2} \leq \frac{s_1}{s_0} \leq u_0^2. \tag{3.4}$$

Therefore one obtains (the worst case is when the ratio is at any extreme):

$$\frac{G(s_0, s_1)}{A(s_0, s_1)} \geq \frac{2u_0}{1 + u_0^2}, \tag{3.5}$$

and the result follows. □

Remark 3.5. A similar argument to that of Lemma 3.4 shows that for any $(z_0, z_1) \in \mathcal{H} \times \mathcal{H}$ there exists $\gamma \in \tilde{\Gamma}$ such that

$$\left(\Im(\gamma_0 z_0)\Im(\gamma_1 z_1)\right)^{1/2} \geq \frac{\sqrt{u_0}}{C_F(1 + u_0)}.$$

Indeed, in this case one can improve (3.4) to

$$u_0^{-1} \leq \frac{y_1}{y_0} \leq u_0$$

by using the action of $\tilde{\gamma}_u = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \in \tilde{\Gamma}$. We will apply this remark to the computation of ATR points, because the integrals $\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f^+$ are $\tilde{\Gamma}$-invariant, and then we can take ϵ_F in Theorem 3.1 to be

$$\epsilon_F = \frac{\sqrt{u_0}}{C_F(1+u_0)}. \tag{3.6}$$

Given $x, y \in \mathcal{H}$ denote by $\rho(x,y)$ the geodesic in $\mathcal{H}$ joining x and y. We also let $d(x,y)$ be the *hyperbolic distance* between x and y. This distance is invariant under the action of $\mathrm{SL}_2(\mathbb{R})$, and it is given by the formula

$$\cosh d(x,y) = 1 + \frac{\mid x - y \mid^2}{2\Im(x)\Im(y)}.$$

Observe that

$$d(x,y) \geq \cosh^{-1}\left(1 + \frac{(\Im(x)/\Im(y) - 1)^2}{2\Im(x)/\Im(y)}\right). \tag{3.7}$$

For $x_0, y_0, x_1, y_1 \in \mathcal{H}$ we denote by $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$ the image under the quotient map $\mathcal{H}^2 \sqcup \{\infty\} \to \Gamma \setminus (\mathcal{H}^2 \sqcup \{\infty\})$ of the region $\rho(x_0,y_0) \times \rho(x_1,y_1) \subset \mathcal{H} \times \mathcal{H}$. Since $\mathrm{SL}_2(\mathbb{R})$ acts by isometries on $\mathcal{H}$ we have that $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} \gamma_0 y_0 & \gamma_1 y_1 \\ \gamma_0 x_0 & \gamma_1 x_1 \end{smallmatrix} \right\}$ for all $\gamma \in \Gamma$ and the *area* of $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$ is given by $d(x_0,y_0)d(x_1,y_1)$.

For a given $\epsilon_0 < \epsilon_F$, let $\epsilon_1 := \sqrt{\epsilon_0 \epsilon_F}$. This auxiliary quantity will be used in the proof of Theorem 3.1. We also define quantities d_0, d_1 and $d_{\min}$ as

$$d_i = \cosh^{-1}\left(1 + \frac{((\epsilon_F/\epsilon_i)^2 - 1)^2}{2(\epsilon_F/\epsilon_i)^2}\right) \text{ for } i \in \{0,1\}, \text{ and } d_{\min} = \min\{d_1, d_2\}.$$

Lemma 3.6. *Let $x_0, y_0, x_1, y_1 \in \mathcal{H}$ be such that $\epsilon(x_0,y_0,x_1,y_1) < \epsilon_0 < \epsilon_F$. Then $\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f$ can be written as a sum of either two or three integrals along sub-regions of $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$ with zero-measure intersection, in which the first one is of the form $\int_{x_0'}^{y_0'}\int_{x_1'}^{y_1'} \omega_f$ with x_0', y_0', x_1', y_1' satisfying the following properties:*

(1) $\epsilon(x_0', y_0', x_1', y_1') \geq \epsilon_0$
(2) for each $i \in \{0,1\}$ either $(x_i', y_i') = (x_i, y_i)$ or $d(x_i', y_i') \geq d_{min}$;

Proof. Actually we will prove that x_0', y_0', x_1', y_1' can be chosen to satisfy

$$\Im(x_0')\Im(x_1') \geq \epsilon_F^2,\ \Im(x_0')\Im(y_1') \geq \epsilon_1^2,\ \Im(y_0')\Im(y_1') \geq \epsilon_0^2,\ \Im(y_0')\Im(x_1') \geq \epsilon_0^2. \tag{3.8}$$

Observe that (3.8) implies condition *(1)* of the lemma.

By Lemma 3.4 and transforming the limits x_0, y_0, x_1, y_1 of the integral under an appropriate element of Γ, we can assume that

$$\Im(x_0)\Im(x_1) \geq \epsilon_F^2. \tag{3.9}$$

If $\Im(x_0)\Im(y_1) \geq \epsilon_1^2$, $\Im(x_1)\Im(y_0) \geq \epsilon_1^2$ and $\Im(y_0)\Im(y_1) \geq \epsilon_1^2$ then $\epsilon(x_0,y_0,x_1,y_1) > \epsilon_0$. So we can suppose that one of these conditions is not satisfied. We divide the proof in three cases, that we label (a), (b) and (c), according to the condition which is not satisfied.

(a) If $\Im(x_0)\Im(y_1) < \epsilon_1^2$. Then we break the integral as

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1}\omega_f = \int_{x_0}^{y_0}\int_{x_1}^{t_1}\omega_f + \int_{x_0}^{y_0}\int_{t_1}^{y_1}\omega_f, \tag{3.10}$$

where $t_1 \in \rho(x_1, y_1)$ satisfies that

$$\Im(t_1)\Im(x_0) = \epsilon_1^2. \tag{3.11}$$

Observe that this is possible because $\Im(x_1) \geq \frac{\epsilon_F^2}{\Im(x_0)} > \frac{\epsilon_1^2}{\Im(x_0)}$ and $\Im(y_1) < \frac{\epsilon_1^2}{\Im(x_0)}$, so that the geodesic between x_1 and y_1 in $\mathcal{H}_1$ intersects the line $\Im(z) = \frac{\epsilon_1^2}{\Im(x_0)}$, and we take t_1 to be the intersection point.

If $\Im(y_0)\Im(t_1) \geq \epsilon_0^2$ then multiplying this condition by (3.9) and using (3.11) we obtain that $\Im(x_1)\Im(y_0) \geq \epsilon_0^2$ and (3.8) holds. Moreover, dividing (3.9) by (3.11) we find that

$$\Im(x_1)/\Im(t_1) \geq (\epsilon_F/\epsilon_1)^2$$

so that, in view of (3.7), the first integral satisfies condition *(2)*.

If $\Im(y_0)\Im(t_1) < \epsilon_0^2$ then we break (3.10) as

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1}\omega_f = \int_{x_0}^{t_0}\int_{x_1}^{t_1}\omega_f + \int_{t_0}^{y_0}\int_{x_1}^{t_1}\omega_f + \int_{x_0}^{y_0}\int_{t_1}^{y_1}\omega_f, \tag{3.12}$$

where we take $t_0 \in \rho(x_0, y_0)$ such that

$$\Im(t_0)\Im(t_1) = \epsilon_0^2. \tag{3.13}$$

This is possible because $\Im(x_0) = \frac{\epsilon_1^2}{\Im(t_1)} > \frac{\epsilon_0^2}{\Im(t_1)}$ and $\Im(y_0) < \frac{\epsilon_0^2}{\Im(t_1)}$. Now multiplying (3.9) and (3.13) and using (3.11) we obtain that $\Im(x_1)\Im(t_0) \geq \epsilon_0^2$. In addition, dividing (3.9) by (3.13) we find that

$$\Im(x_0)/\Im(t_0) \geq (\epsilon_F/\epsilon_0)^2,$$

which implies condition *(2)* for the first integral.

(b) If $\Im(x_1)\Im(y_0) < \epsilon_1^2$. This is analogous to the first case: we break the integral as

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1}\omega_f = \int_{x_0}^{t_0}\int_{x_1}^{y_1}\omega_f + \int_{t_0}^{y_0}\int_{x_1}^{y_1}\omega_f, \tag{3.14}$$

where $t_0 \in \rho(x_0, y_0)$ satisfies that $\Im(t_0)\Im(x_1) = \epsilon_1^2$. If $\Im(t_0)\Im(y_1) < \epsilon_0^2$ then we break further the integral as

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1}\omega_f = \int_{x_0}^{t_0}\int_{x_1}^{t_1}\omega_f + \int_{x_0}^{t_0}\int_{t_1}^{y_1}\omega_f + \int_{t_0}^{y_0}\int_{x_1}^{y_1}\omega_f, \tag{3.15}$$

where we take $t_1 \in \rho(x_1, y_1)$ such that $\Im(t_0)\Im(t_1) = \epsilon_0^2$.

(c) If $\Im(y_0)\Im(y_1) < \epsilon_1^2$. In this case we can assume that

$$\Im(x_0)\Im(y_1) \geq \epsilon_1^2 \quad \text{and} \quad \Im(x_1)\Im(y_0) \geq \epsilon_1^2, \tag{3.16}$$

because otherwise we are in case (a) or (b). Then we can also suppose that

$$\Im(y_0)\Im(y_1) < \epsilon_0^2, \tag{3.17}$$

because otherwise $\epsilon(x_0, y_0, x_1, y_1) \geq \epsilon_0$. Then we can break the integral as

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1}\omega_f = \int_{x_0}^{t_0}\int_{x_1}^{y_1}\omega_f + \int_{t_0}^{y_0}\int_{x_1}^{y_1}\omega_f,$$

where $t_0 \in \rho(x_0, y_0)$ satisfies that

$$\Im(t_0)\Im(y_1) = \epsilon_0^2. \tag{3.18}$$

Observe that

$$\Im(t_0)\Im(x_1) = \frac{\epsilon_0^2 \Im(x_1)}{\Im(y_1)} > \Im(y_0)\Im(x_1) \geq \epsilon_1^2,$$

so that the first integral satisfies the conditions of the Lemma, because from (3.16) and (3.18) if follows that $\Im(x_0)/\Im(t_0) \geq (\epsilon_1/\epsilon_0)^2 = (\epsilon_F/\epsilon_1)^2$.

□

Proof of Theorem 3.1. Define the quantity $\epsilon(I)$ as

$$\epsilon(I) = \epsilon(x_0, y_0, x_1, y_1), \text{ if } I = \int_{x_0}^{y_0} \int_{x_1}^{y_1} \omega_f.$$

We can compute an expression $I = I_1 + \cdots + I_n$ with $\epsilon(I_i) \geq \epsilon_0$ as in (3.3) by repeated application of Lemma 3.6. To be more precise, we can apply the following algorithmic procedure.

We initialize a void list V and a list $W = [I]$. We denote by W_0 the first element in W. If $\epsilon(W_0) \geq \epsilon_0$ we append W_0 to V and we remove W_0 from W. If $\epsilon(W_0) < \epsilon_0$, we apply Lemma 3.6 to write $W_0 = I_0 + J_1 + \cdots + J_k$ with $\epsilon(I_0) \geq \epsilon_0$ and $k \leq 2$. We append I_0 to V, we remove W_0 from W and we append $J_1, \ldots, J_k$ to W. Then we repeat the process to the first element W_0 in the list W, until W is void.

Observe that if this process finishes in a finite number of steps, then at the end the list V contains integrals $I_0, I_1, \ldots, I_n$ with $I = I_0 + \cdots + I_n$ and $\epsilon(I_i) \geq \epsilon_0$ for all $i = 1, \ldots, n$, as desired. What remains to be shown, then, is that this procedure cannot be repeated infinitely many times. As we shall now see, this follows from properties *(2)* and *(3)* of Lemma 3.6.

First of all, observe that I is the integral of ω_f along the region $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$. Applying Lemma 3.6 to a certain integral $W_0 = \int_{r_0}^{s_0} \int_{r_1}^{s_1} \omega_f$ amounts to give a decomposition of the region $\left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\} \subseteq \left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$ into a union of regions with zero measure intersection. This decomposition can be of the following 4 types, which correspond to (3.12), (3.15), (3.10) and (3.14) respectively:

(i) $\left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} t_0 & t_1 \\ r_0 & r_1 \end{smallmatrix} \right\} \sqcup \left\{ \begin{smallmatrix} y_0 & t_1 \\ t_0 & r_1 \end{smallmatrix} \right\} \sqcup \left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & t_1 \end{smallmatrix} \right\}$ with $d(r_i, t_i) > d_{\min}$ for $i = 0, 1$,
(ii) $\left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} t_0 & t_1 \\ r_0 & r_1 \end{smallmatrix} \right\} \sqcup \left\{ \begin{smallmatrix} t_0 & r_1 \\ r_0 & t_1 \end{smallmatrix} \right\} \sqcup \left\{ \begin{smallmatrix} s_0 & s_1 \\ t_0 & r_1 \end{smallmatrix} \right\}$ with $d(r_i, t_i) > d_{\min}$ for $i = 0, 1$,
(iii) $\left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} s_0 & t_1 \\ r_0 & r_1 \end{smallmatrix} \right\} \sqcup \left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & t_1 \end{smallmatrix} \right\}$ with $d(r_1, t_1) > d_{\min}$, or
(iv) $\left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} t_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\} \sqcup \left\{ \begin{smallmatrix} s_0 & s_1 \\ t_0 & r_1 \end{smallmatrix} \right\}$ with $d(r_0, t_0) > d_{\min}$.

Each time that an application of Lemma 3.6 gives a decomposition of type (i) or (ii), the first term is a subregion of $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$ of area at least $d_{\min}^2$. Since the area of $\left\{ \begin{smallmatrix} y_0 & y_1 \\ x_0 & x_1 \end{smallmatrix} \right\}$ is finite, this cannot happen infinitely many times. Therefore, in the algorithmic process described above we can assume that, after a finite number of steps, all applications of Lemma 3.6 give rise to decompositions of types (iii) or (iv).

At this stage, the algorithmic procedure applied to an integral W_0 is as follows. Let $R_0 = \left\{ \begin{smallmatrix} s_0 & s_1 \\ r_0 & r_1 \end{smallmatrix} \right\}$ be the region associated to W_0, and let $\Delta(R_0) = d(r_0, s_0) + d(r_1, s_1)$. As application of Lemma 3.6 one obtains a decomposition $R_0 = R_1 \sqcup S_1$ of type (iii) or (iv). Observe that $\Delta(S_1) \leq \Delta(R_0) - d_{\min}$ by property *(3)* of Lemma 3.6. If $\epsilon(S_1) \geq \epsilon_0$ then procedure for W_0 ends; otherwise one iterates by applying again 3.6, obtaining $S_1 = R_2 \sqcup S_2$ with $\Delta(S_2) \leq \Delta(S_1) - d_{\min}$. It is clear

that this procedure cannot continue indefinitely because $\Delta(S_i) \geq 0$. Therefore, at some step $\epsilon(S_i) \geq \epsilon_0$ and the process for W_0 ends.

4. Dependence on the continued fractions

The computation of ATR points is equivalent to the computation of semi-definite integrals of the form

$$\int^{\tau_0} \int_{\infty}^{c} \omega_f^+, \quad c \in F. \tag{4.1}$$

As we recalled in §2.2, one can write (4.1) as a sum of ordinary 4-limit integrals by expressing c as a continued fraction with coefficients in $\mathcal{O}_F$. If the limits of the resulting ordinary integrals are too close to the real axis then the number of terms to sum for a prescribed accuracy, and therefore the number of Fourier coefficients to be computed, may be too large. In this case, the algorithm described in §3 can be used to express them as sums of integrals whose limits are uniformly bounded away from the real axis, reducing the number of terms and Fourier coefficients needed.

If F is norm-euclidean then the euclidean algorithm gives an effective procedure for computing continued fractions. This is the method used in the numerical calculations over $\mathbb{Q}(\sqrt{29})$, $\mathbb{Q}(\sqrt{37})$ and $\mathbb{Q}(\sqrt{41})$ carried out in [DL03]. But this can only be done in a few fields: there are only finitely many norm-euclidean real quadratic fields, being $\mathbb{Q}(\sqrt{73})$ the one having largest discriminant.

An algorithm for computing continued fractions in 2-stage euclidean real quadratic fields was given in [GM12]. A field F is said to be 2-*stage euclidean* if for every $a, b \in \mathcal{O}_F$, $b \neq 0$, there exist either:

(i) $q, r \in \mathcal{O}_F$ with $a = qb + r$ and $\mathrm{Nm}(r) < \mathrm{Nm}(b)$, or
(ii) $q_1, q_2, r_1, r_2 \in \mathcal{O}_F$ with $a = q_1 b + r_1, \quad b = q_2 r_1 + r_2$ and $\mathrm{Nm}(r_2) < \mathrm{Nm}(b)$.

All real quadratic fields of class number 1 are conjectured to be 2-stage euclidean (see [Coo76]). Actually, the algorithm of [GM12] can also be used to verify that a given F is 2-stage euclidean, and this was used to prove that all real quadratic fields of class number 1 and discriminant up to $8,000$ are indeed 2-stage euclidean [GM12, Theorem 4.1].

Unlike the situation encountered in norm-euclidean fields, 2-stage division chains as in condition (ii) are not unique. As a consequence, elements of F admit in general many different continued fraction expansions. This leads to different expressions of (4.1) as a sum of ordinary integrals, whose limits may have very different imaginary parts. As it will be illustrated in §5 with some explicit examples, numerical experiments suggest that it is useful to exploit non-uniqueness of continued fractions, by searching for continued fractions leading to integrals whose limits have large imaginary parts; or, to be more precise, whose limits give large values of the quantity ϵ defined in (3.2). The procedure for computing an expression such as (4.1) is then:

(1) Compute all continued fraction expansions of c given by the algorithm of [GM12], which have length up to a certain fixed bound.
(2) For each continued fraction, compute the corresponding expression of (4.1) as a sum of ordinary integrals and compute $\epsilon_{\min}$: the minimum of the quantities ϵ corresponding to the limits.
(3) Choose the continued fraction giving the highest $\epsilon_{\min}$.

(4) For each of the ordinary integrals appearing in the expression given by the continued fraction found in the previous step, compute the quantity ϵ and apply the algorithm of Theorem 3.1 if $\epsilon < \epsilon_F$, with a suitable choice of $\epsilon < \epsilon_0 < \epsilon_F$.

We end the section with some remarks about the algorithm above.

1. One can exploit non-uniqueness of 2-stage division chains even if F is euclidean. As the next section illustrates, this may be beneficial since it usually gives rise to integrals with larger values of ϵ, providing an improvement even on the curves already considered in [DL03]. In some cases, it may even happen that the $\epsilon_{\min}$ obtained in this way is higher than ϵ_F, in which case it is not necessary to apply the algorithm provided by Theorem 3.1. However, the lack of an a priori estimate of the value $\epsilon_{\min}$ obtained by the non-uniqueness of division chains trick explains the key importance of Theorem 3.1 in treating the cases where $\epsilon_{\min} < \epsilon_F$.
2. In Step (3) we choose the continued fraction giving the highest $\epsilon_{\min}$ because experimentally this seems to produce the fewer resulting integrals in step (4). We have no rigorous explanation for this fact, although it seems reasonable that better initial conditions give better results.
3. There is a trade-off between small and large values of ϵ_0 in Step (4) above: smaller values yield less integrals after the breaking process, but each of these integrals requires more Fourier coefficients at the time of integration; on the other hand, higher values lead to integrals requiring less Fourier coefficients, but the number of resulting integrals tends to be higher. Experimentally, we found that the running time of the algorithm is more sensible to the number of needed Fourier coefficients, so a value of ϵ_0 close to ϵ_F seems to be a good choice. For instance, in the implementation of the algorithm used to compute the numerical examples of the next section, we used $\epsilon_0 = 0.81\epsilon_F$, which corresponds to a value of $\epsilon_1 = 0.9\epsilon_F$.

5. Numerical verification of Darmon's conjecture

In this section we illustrate the algorithm described above by calculating approximations to ATR points which add numerical evidence on top of the one presented in [DL03]. Before detailing the computation of an ATR point on E_{509}, we comment on some calculations of ATR points on three $\mathbb{Q}$-curves that we denote E_{29}, E_{37}, and E_{109}. The curves E_{29} and E_{37} were also considered in [DL03], and we have included them here in order to compare the computational requirements of the algorithm used in [DL03] with the one presented in this note. The curve E_{109} is an example of a curve of conductor 1 defined over a real quadratic field of class number 1 which is not norm-euclidean. Therefore, it was not numerically accessible before, although it is a $\mathbb{Q}$-curve and algebraic points can be more efficiently computed by using the Heegner point method of [DRZ12].

The computations for E_{29}, E_{37}, and E_{109} were performed on a laptop with *Intel Core^{TM} i5-2540M* CPU running at 2.60 GHz, and 8 GB of memory. For the curve E_{509} we used a machine equipped with eight *Quad-Core AMD Opteron^{TM} Processor 8384* for a total of 32 cores running each at 800 MHz, and equipped with 320 GB of memory.

The curve E_{29}. Consider the curve defined over $F = \mathbb{Q}(\sqrt{29})$ and given by the equation

$$E_{29}\colon y^2 + xy + (5\omega + 11)y = x^3, \quad \omega = \frac{1+\sqrt{29}}{2}.$$

For this field the estimated C_F is $C_F \simeq 5$ (see Remark 3.3), which by (3.6) yields $\epsilon_F \simeq 0.0736$.

We consider the ATR field $K = F(\beta)$ with $\beta = \sqrt{9\omega + 3}$, for which $E_{29}(K)$ has a non-torsion point with x-coordinate equal to $-1/3$. With the algorithm used in [DL03], one obtains integrals with $\epsilon_{\min} \simeq 0.00145$. In order to get 12 decimal digits, which is the minimum precision in which the calculations in [DL03] were performed, one would have needed to find the Fourier coefficients of all ideals up to norm $N \simeq 6.7 \cdot 10^7$.

Using the non-uniqueness of continued fraction expansions as explained in Section 4, considering expansions of length up to 5, we obtained 5 integrals with imaginary part $\epsilon_{\min} \simeq 0.0072$, which is almost 5 times better than before. In order to obtain the same precision one would have to find the Fourier coefficients of ideals up to norm $N \simeq 2.7 \cdot 10^6$, which is almost 25 times less.

Since $\epsilon_{\min} < \epsilon_F$, we broke further the integrals with the algorithm of Theorem 3.1 to move the imaginary parts of the limits close to this theoretical optimal, with a choice of $\epsilon_0 = 0.81\epsilon_F$ in Step (4) of the algorithm outlined in Section 4. This yielded 539 integrals with an imaginary part of $\epsilon_{\min} \simeq 0.0596$, and allowed us to obtain the same precision of 12 digits by only considering ideals up to norm $N \simeq 40,000$: an improvement by a factor of $1,675$. By taking ideals of norm up to $40,000$ we obtained that

$$J_\tau = 13.2923360157968468468\ldots - 10.78402031269077180934\ldots i,$$

and $-3 \cdot J_\tau$ coincides with P up to the prescribed accuracy. The calculation took less than two minutes.

The curve E_{37}. Let E_{37} be the curve defined over $F = \mathbb{Q}(\sqrt{37})$ appearing in [DL03] and having equation

$$E_{37}\colon y^2 + y = x^3 + 2x^2 - (19 + 8\omega)x + 28 + 11\omega, \quad \omega = \frac{1+\sqrt{37}}{2}.$$

For this field the constant C_F is approximately equal to 6. By (3.6) we see that $\epsilon_F \simeq 0.044$.

We consider the field $K = F(\beta)$, with $\beta = \sqrt{4\omega + 10}$, and one of the points computed by [DL03], namely

$$P = (-\beta^2/8 - 3/4, -\beta^3/8 - 1/2).$$

Using the algorithm of [DL03] one obtains a minimal imaginary part of $\epsilon_{\min} \simeq 0.0012$, which means that one has to integrate using the Fourier coefficients up to norm $N \simeq 1.12 \cdot 10^8$ for obtaining 12 digits of precision.

In order to illustrate the algorithm of Theorem 3.1 we rewrote the integrals provided by the method of [DL03] as a sum involving 328 integrals (with a choice of $\epsilon_0 = 0.81\epsilon_F$). The minimal imaginary part then improved to $\epsilon_{\min} \simeq \epsilon_0 \simeq 0.0359$, which means that to get 12 digits of precision it is enough to use ideals of norm up to $N \simeq 138,000$. This is an improvement by a factor of 815. In this case, it took about 7 minutes to find that

$$J_\tau = -1.3589031642485772101\ldots + 8.36575277665729384437\ldots i,$$

which satisfies the equality

$$5J_\tau \stackrel{?}{=} -8P$$

up to the prescribed accuracy.

The curve E_{109}. In the two remaining subsections we present larger examples that were not available to [DL03]. First, consider the curve E_{109} defined over the field $F = \mathbb{Q}(\sqrt{109})$, and given by the equation

$$E_{109}\colon y^2 + \omega xy = x^3 - (1+\omega)x^2 - (58\omega + 245)x - 630\omega - 2944, \quad \omega = \frac{1+\sqrt{109}}{2}$$

Although E_{109} is a $\mathbb{Q}$-curve, the field F is not norm-euclidean and therefore this example was not available before. For this field we have that $C_F \simeq 10.4$, giving that $\epsilon_F \simeq 0.006$. By using the algorithm of Theorem 3.1 with, say, $\epsilon_0 = 0.81\epsilon_F$, one can express any integral $\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f^+$ as a sum of integrals with $\epsilon \simeq 0.81 \cdot \epsilon_F \simeq 0.0048$. In order to compute any such integral with $\epsilon = 0.0048$ to a precision of 12 digits, one needs to sum the Fourier coefficients of norm up to roughly $2 \cdot 10^7$.

Let us consider the point $P = (3\omega + 11, \frac{1}{2}\beta - 7\omega - 81/2)$ defined over the field $K = F(\beta)$, with $\beta = \sqrt{268\omega + 1265}$. Exploiting the non-uniqueness of continued fractions, and considering expansions of length up to 5, we obtained 8 integrals with $\epsilon_{\min} \simeq 0.035$, which is roughly 6 times higher than ϵ_F. It is not necessary then in this case to further break the integrals. We computed an approximation to the ATR point by considering ideals of norm up to $N = 430,000$, obtaining that

$$J_\tau = -3.24024368505944150\ldots \cdot 10^{-12} - 42.392087963225793791\ldots i,$$

which satisfies

$$J_\tau \stackrel{?}{=} -2P$$

up to the prescribed precision of 12 digits. This computation took less than 3 minutes.

The curve E_{509}. We consider here the curve already mentioned in Section 1 and in [DL03], defined over $F = \mathbb{Q}(\sqrt{509})$ and given by the equation

$$y^2 - xy - \omega y = x^3 + (2+2w)x^2 + (162+3w)x + (71+34\omega), \quad \omega = \frac{1+\sqrt{509}}{2}.$$

We have that $C_F \simeq 22.5$, and therefore $\epsilon_F \simeq 0.0015$. Theorem 3.1 allows us to express any integral $\int_{x_0}^{y_0}\int_{x_0}^{y_0} \omega_f^+$ as a sum of integrals having $\epsilon < \epsilon_0 < \epsilon_F$. For instance, for a choice of $\epsilon_0 = 0.81\epsilon_F$ we obtain that each of those integrals could be computed to 12 digits of precision by summing over the Fourier coefficients of norm up to roughly $1.6 \cdot 10^9$; a bound which, although being large, is within reach of the current technology.

We consider the ATR field $K = F(\beta)$ where $\beta = \sqrt{9144\omega + 98577}$, and the point $P \in E(K)$ of infinite order having coordinates

$$P = (\omega + 17, \beta/2 + \sqrt{509}/2 + 9).$$

The field extension K/F has relative discriminant of norm 55, which is relatively small. Write

$$\mathcal{O}_K = \mathcal{O}_F + \alpha\mathcal{O}_F, \quad \alpha^2 + \alpha = 127\sqrt{509} + 2865.$$

The ATR points are conjectured to be defined over the Hilbert class field of K. Since K has class number 2, we will need to compute the points corresponding to

the two non-equivalent optimal embeddings if we want to obtain a point defined over K. The first of these embeddings maps

$$\alpha \mapsto \varphi_1(\alpha) = \begin{pmatrix} 0 & 254\omega + 2738 \\ 1 & -1 \end{pmatrix},$$

whereas the second maps

$$\alpha \mapsto \varphi_2(\alpha) = \begin{pmatrix} 0 & 127\omega + 1369 \\ 2 & -1 \end{pmatrix}.$$

The fixed points for the induced action of $K^\times$ on $\mathcal{H}$ given by the embedding $v_0 \colon K \hookrightarrow \mathbb{C}$ are, respectively:

$$\tau_0^{(1)} = 0.5 + 0.024492046328012136937583\ldots i$$
$$\tau_0^{(2)} = \frac{1}{2}\tau_0^{(1)}.$$

Exploiting the non-uniqueness of quadratic continued fractions we obtain 4 integrals for the first of the points, and 8 for the second. The then minimal imaginary parts are $\epsilon_{\min}^{(1)} = 0.01917$ and $\epsilon_{\min}^{(2)} = 0.002926$. Since $\epsilon_{\min}^{(1)} > \epsilon_F$ and $\epsilon_{\min}^{(2)} > \epsilon_F$ we see that in this case it is not necessary to break further the integrals using Theorem 3.1.

In order to obtain about 12 decimal digits of accuracy we precomputed the Fourier coefficients of all ideals up to norm $4 \cdot 10^8$. The total computation time was under two days on the 32-processor machine specified at the beginning of this section. We should note that in this computation we heavily exploited parallelism, both when computing the Fourier coefficients as well as during the integration step. The period lattices for E_K attached to the Néron differential $\omega_{E_K} = \frac{dx}{2y-x-\omega}$ are

$$\Lambda_0 = \langle -5.38425378853615683456\ldots, -7.44383552310672504690\ldots i\rangle = \langle \lambda_0^+, \lambda_0^-\rangle,$$
$$\Lambda_1 = \langle 2.47855898378449003059\ldots, 1.14589256545011559322\ldots i\rangle = \langle \lambda_1^+, \lambda_1^-\rangle.$$

A preimage of P on $\mathbb{C}/\Lambda_0$ under the Weierstrass map is

$$z = -2.69212689426807841728 34\cdots - 5.14260865315735723708 22\ldots i.$$

The computed values are

$$J_\tau^{(1)} = 22.6329152877266950421310249 8\ldots i,$$
$$J_\tau^{(2)} = 106.76152478838805709877318 8\ldots - 73.61795079733479815342402 51\ldots i.$$

Setting $J_\tau = J_\tau^{(1)} + J_\tau^{(2)}$ we find that:

$$\left| \frac{J_\tau}{\lambda_1^+} - 4z + 10\lambda_0^+ \right| \simeq 5.126285 \cdot 10^{-11},$$

which suggests that

$$J_\tau \stackrel{?}{=} 4z.$$

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 1839918 (2002d:11058)

[BR07] Matthias Beck and Sinai Robins, *Computing the continuous discretely*, Undergraduate Texts in Mathematics, Springer, New York, 2007, Integer-point enumeration in polyhedra. MR 2271992 (2007h:11119)

[Coo76] George E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I*, J. Reine Angew. Math. **282** (1976), 133–156. MR 0406973 (53 #10758a)

[Dar01] Henri Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*, Ann. of Math. (2) **154** (2001), no. 3, 589–639. MR 1884617 (2003j:11067)

[Dar04] ———, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR 2020572 (2004k:11103)

[Das05] Samit Dasgupta, *Stark-Heegner points on modular Jacobians*, Ann. Sci. École Norm. Sup. (4) **38** (2005), no. 3, 427–469. MR 2166341 (2006e:11080)

[Dem08] Lassina Dembélé, *An algorithm for modular elliptic curves over real quadratic fields*, Experiment. Math. **17** (2008), no. 4, 427–438. MR 2484426 (2010a:11119)

[DL03] Henri Darmon and Adam Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*, Int. Math. Res. Not. (2003), no. 40, 2153–2180. MR 1997296 (2005f:11110)

[DRZ12] Henri Darmon, Victor Rotger, and Yu Zhao, *The Birch and Swinnerton-Dyer conjecture for $\mathbb{Q}$-curves and Oda's period relations*, 1–40.

[Fre90] Eberhard Freitag, *Hilbert modular forms*, Springer-Verlag, Berlin, 1990. MR 1050763 (91c:11025)

[Gär11a] Jérôme Gärtner, *Darmon's points and quaternionic Shimura varieties*, Arxiv preprint arXiv:1104.3338 (2011).

[Gär11b] ———, *Points de Darmon et variétés de Shimura*, 2011.

[GM12] Xavier Guitart and Marc Masdeu, *Computing continued fractions on real quadratic fields*, Mathematics of Computation **0** (2012).

[Gre09] Matthew Greenberg, *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*, Duke Math. J. **147** (2009), no. 3, 541–575. MR 2510743 (2010f:11097)

[GRZ12] Xavier Guitart, Victor Rotger, and Yu Zhao, *Almost totally complex points on elliptic curves*, Arxiv preprint arXiv:1204.3402 (2012).

[Lon06] Matteo Longo, *On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 3, 689–733. MR 2244227 (2008f:11071)

[LRV09] Matteo Longo, Victor Rotger, and Stefano Vigni, *On rigid analytic uniformizations of Jacobians of Shimura curves*, Arxiv preprint arXiv:0910.3391 (2009).

[SW01] Christopher M. Skinner and Andrew J. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse Math. (6) **10** (2001), no. 1, 185–215. MR 1928993 (2004b:11073)

[Wil95] Andrew J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 1333035 (96d:11071)

Universitat Politècnica de Catalunya, Barcelona
Max Planck Institute for Mathematics, Bonn
E-mail address: xevi.guitart@gmail.com

Columbia University, New York
E-mail address: masdeu@math.columbia.edu